第6章　合同式の応用，剰余類

6.1　合同式の簡単な応用

[I]　足し算，引き算，掛け算については，法 m によって合同な数は “同じ数” と思って計算してよい，というのが合同式の計算法である（割り算については注意が必要であった）．また，$m \geq 2$ ならば，すべての整数は m を法 として 0 以上 m 未満の整数と合同だから，合同式の計算は m 未満の整数の演算に帰着できる．これにより，大きな整数に関する計算も，合同式として扱えば簡単になる場合がある．

例 6.1　5432^{19876} を 19 で割った余りはいくつか？　直接 5432^{19876} を計算するのは現実には不可能である．そこで，まず $5432 \equiv 17 \equiv -2 \pmod{19}$ より $(-2)^{19876}$ の計算に帰着させる．ここで，$(-2)^9 = -2 \cdot (2^4)^2 = -2 \cdot 16^2 \equiv -2 \cdot (-3)^2 = -18 \equiv 1 \pmod{19}$ に注目する．そこで，$19876 \equiv 4 \pmod{9}$ から，$19876 = 4 + 9k$ $(k \in \boldsymbol{Z})$ と書けて，

$$5432^{19876} \equiv (-2)^{19876} = (-2)^{4+9k} = (-2)^4 \cdot (-2)^{9k} \equiv 16 \cdot 1 = 16 \pmod{19}.$$

したがって余りは 16 である．

[II]　上の計算で，$19876 \equiv 4 \pmod{9}$ については，実際には割り算をしなくても，各桁の数を足していくだけで確かめられる．

$$19876 \longrightarrow 1+9+8+7+6 = 31 \longrightarrow 3+1 = 4 \quad \text{より} \quad 19876 \equiv 4 \pmod{9}.$$

この方法の有効性を一般的に検証するために，自然数 a を 10 進展開したときの各桁を加えて得られる自然数を $D(a)$ とする．たとえば，$D(19876) = 31$，$D(65228) = 23$ である．一般に，自然数 a の各桁が $a_0, a_1, a_2, \cdots, a_N$ (a_k は 10^k の位の数) のとき，

$$a = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_N \times 10^N, \quad D(a) = a_0 + a_1 + a_2 + \cdots + a_N$$

であるが，$10 \equiv 1 \pmod{9}$ より，$a \equiv D(a) \pmod{9}$ を得る．さらに，D の計算を少し修正して，a の各桁を加える過程で 9 になったら 0 とみなすことにし，一桁の数になるまでこれを繰り返して，その結果を $\bar{D}(a)$ で表せば，$D(a) \equiv \bar{D}(a) \pmod{9}$，したがって次の命題が証明された．

命題 6.2　任意の自然数 a に対して，$a \equiv \bar{D}(a) \pmod{9}$．

とくに，a が 9 で割り切れるためには $\bar{D}(a)=0$ が必要十分である． $10\equiv 1 \pmod 3$ より，上の議論は 3 の倍数の判定にも使える． すなわち，a の各桁を ($3,6,9$ が現れたら 0 とみなして) 足すことを一桁の数になるまで繰り返し，その結果を $\bar{D}'(a)$ とすれば，$a\equiv \bar{D}'(a) \pmod 3$ となる． これにより，3 の倍数かどうかの簡単な判定法が得られる．

さらに，$\bar{D}$ の計算によって古代から知られている**九去法**という検算法が説明できる． すなわち，自然数の足し算 $a+b=c$ を検算したいとき，a,b の各桁をすべて加え 9 が現われたら 0 とみなすことを繰り返し，c についても同様にして，両辺とも一桁の数にする． 得られた数が異なれば元の計算は間違いだと推論できる． これが九去法である． この検算法の原理は，ＩＴ技術においてデータ転送の信頼性を高めるために，**誤り検出符号** (チェックサム) として現在広く使われている．

[III]　平方数が合同式でどのようにふるまうか調べてみる． まず，最も簡単なケースとして 4 を法とする場合を考える． a が偶数ならば明らかに $a^2\equiv 0 \pmod 4$ であり，奇数ならば $a\equiv \pm 1 \pmod 4$ より $a^2\equiv 1 \pmod 4$ である． さらに強く，次が成り立つ．

命題 6.3 整数 a に対して，

$$a^2 \equiv \begin{cases} 0 \pmod 4 & (a：偶数), \\ 1 \pmod 8 & (a：奇数). \end{cases}$$

証明　a が偶数ならば，$a^2=(2n)^2=4n^2\equiv 0 \pmod 4$ よりＯＫなので，以下，a を奇数とする． このとき $a\equiv \pm 1 \pmod 4$ をみたすから $a=\pm 1+4k$ ($k\in \boldsymbol{Z}$) と書ける． よって $a^2=1\pm 8k+16k^2\equiv 1 \pmod 8$ となる． □

これを用いて，たとえばピタゴラス方程式の整数解について以下のようなことが示せる．

系 6.4 整数 a,b,c が $a^2+b^2=c^2$ をみたすならば，$ab\equiv 0 \pmod 4$ が成り立つ．

証明　a,b どちらも偶数ならば，$ab\equiv 0 \pmod 4$ が成り立つことは明らかである． よって a,b のどちらかは奇数，たとえば a が奇数とする． このとき b も奇数とすると，

$$c^2=a^2+b^2\equiv 1+1=2 \pmod 4$$

となって前命題と矛盾する． よって b は偶数，c は奇数であり，$b=2b'$ と書けば，

$$4b'^2=b^2=c^2-a^2\equiv 1-1=0 \pmod 8, \qquad \therefore\ b'^2\equiv 0 \pmod 2.$$

よって b' は偶数，したがって b は 4 の倍数であり，とくに $ab\equiv 0 \pmod 4$ を得る． □

以上は 4 または 8 を法として考えたが，3 やそのべきを法とするとき，あるいは 5 やそのべきを法とするとき，平方数はどんな合同式をみたすか考えてみよ．

6.2 剰余類

定義 6.5 整数 m および a に対して，$x \equiv a \pmod m$ をみたす整数 x 全体の集合を $a+m\boldsymbol{Z}$ で表し，**法 m に関する（a の属する）剰余類**という；

$$a+m\boldsymbol{Z} = \left\{ x \in \boldsymbol{Z} \,\middle|\, x \equiv a \pmod m \right\}.$$

$0+m\boldsymbol{Z}$ は $m\boldsymbol{Z}$ のことである． 後の説明にもあるように，m が特定されている場合には $\overline{a}$ と略記することが多い； $\overline{a} = a+m\boldsymbol{Z}$.

次の命題は剰余類の定義から簡単に示すことができる．

命題 6.6 m および a,b,c を整数とする．

(1) $a+m\boldsymbol{Z} = b+m\boldsymbol{Z}$, $(a+m\boldsymbol{Z}) \cap (b+m\boldsymbol{Z}) = \phi$ のどちらか一方が必ず成り立つ．
(2) $b,c \in a+m\boldsymbol{Z}$ ならば $b \equiv c \pmod m$.
(3) 次の 4 つは互いに同値である；

$$a \equiv b \pmod m, \quad a \in b+m\boldsymbol{Z}, \quad b \in a+m\boldsymbol{Z}, \quad a+m\boldsymbol{Z} = b+m\boldsymbol{Z}.$$

前の節のはじめでも述べたように，合同式においては m を法として合同な数を “等しい” とみなして計算する． 法 m で合同な整数をひとまとめにした $\boldsymbol{Z}$ の部分集合が，m を法とする剰余類である． すなわち，合同式における計算とは，剰余類をあたかも数のように扱って行う計算とみなすことができる． これについては，次の節で詳しく述べるので、ちょっと待っててね．

定義 6.7 整数 m に対して，法 m に関するすべての剰余類を元とする集合を**法 m に関する剰余環**といい，$\boldsymbol{Z}/m\boldsymbol{Z}$ で表す；

$$\boldsymbol{Z}/m\boldsymbol{Z} = \{\, a+m\boldsymbol{Z} \mid a \in \boldsymbol{Z} \,\}.$$

さて，しばらくの間，自然数 m を固定し，剰余類 $a+m\boldsymbol{Z}$ を $\overline{a}$ と略す． 法 m に関する剰余類は全部で m 個ある． 実際，すべての整数は m を法として $0,1,2,\cdots,m$ のどれかと合同で，これらは互いに合同でないから

$$\boldsymbol{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{m-1}, \qquad \overline{a} \cap \overline{b} = \phi \quad (0 \le a < b < m).$$

したがって，剰余類は全部で m 個あり，

$$\boldsymbol{Z}/m\boldsymbol{Z} = \left\{ \overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1} \right\}$$

と書くことができる． たとえば，$\boldsymbol{Z}/5\boldsymbol{Z} = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$ であるが，これを，いやだけど

$$\boldsymbol{Z}/5\boldsymbol{Z} = \left\{ \overline{7810}, \overline{-29}, \overline{23+34}, \overline{987-654}, \overline{99^{99}} \right\}$$

と書いてもかまわない（オレを信じちゃいけないぜ，計算して確かめよ）．

6.3　剰余類の和と積

はじめに，合同式に関して

$$a_1 \equiv a_2,\ b_1 \equiv b_2 \pmod{m} \implies a_1 + b_1 \equiv a_2 + b_2,\ a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

が成り立つことに注意しよう（命題 5.2）．このことは，2 つの剰余類からそれぞれの元を選ぶとき，それらの和や積の属する剰余類が選んだ元によらずに定まることを示している．そこで，“剰余類” の “和” や “積” を以下のように定義できることがわかる．

定義 6.8 剰余類 $a + m\boldsymbol{Z}, b + m\boldsymbol{Z} \in \boldsymbol{Z}/m\boldsymbol{Z}$ に対して，それらの和，積を

$$(a + m\boldsymbol{Z}) + (b + m\boldsymbol{Z}) = (a + b) + m\boldsymbol{Z}, \qquad (a + m\boldsymbol{Z})(b + m\boldsymbol{Z}) = (ab) + m\boldsymbol{Z}$$

によって定める．

この定義による和と積は，略記法で

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a}\overline{b} = \overline{ab}$$

と書いても同じである．こう表すとアタリマエのように見えるでしょ？ たとえば，7 を法として $\overline{2} + \overline{3} = \overline{5}$ とか $\overline{2} \cdot \overline{3} = \overline{6}$ など…．一方，$\overline{3} + \overline{5} = \overline{1}$ や $\overline{4} \cdot \overline{6} = \overline{3}$ となると少しはアタリマエじゃなくなる…．剰余類の等式

$$\overline{a} + \overline{b} = \overline{c}, \quad \overline{a}\overline{b} = \overline{d}$$

における和や積は，合同式

$$a + b \equiv c, \quad ab \equiv d \pmod{m}$$

における整数の和，積を，剰余類の和，積とみなして表したもの，と考えればよい．**「合同式」**は**「剰余類における等式」**であり，その意味で，剰余類の演算は合同式に現れる演算を，より直感的に表現していると考えられる．たとえば，未知数 x をもつ合同式

$$ax \equiv b \pmod{m}$$

は，剰余類に関する方程式

$$\overline{a}x = \overline{b}$$

と同等であり，より簡明になる．ただし，未知数 x として，前者の場合は整数を想定するのに対し，後者は剰余類つまり $\boldsymbol{Z}/m\boldsymbol{Z}$ の元を想定するという違いがある．しかし，慣れてくると，これらを同一視してあまり区別せずに議論できるようになる．皆さんも，早く慣れて，自由に使えるようになってくれるといいな．

なお，“$\equiv \pmod{\ }$” を $\boldsymbol{Z}$ 上の**同値関係**とみなし，それによって $\boldsymbol{Z}$ を**同値類別**して得られる**商集合**として $\boldsymbol{Z}/m\boldsymbol{Z}$ をとらえることもできる．この考え方はめっちゃ一般化され，数学のいろんな分野に現れるけど，詳しくは演習の時間にまかせちゃったりして，ずるい？